

Perancangan Kriptografi *Block Cipher* dengan Langkah Permainan Engklek

¹⁾Kismanto Dwi Cahyono, ²⁾Evangs Mailoa

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Jl. Diponegoro 52-60, Salatiga 50771, Indonesia

Email: ¹⁾672010038@student.uksw.edu, ²⁾evangs.mailoa@staff.uksw.edu

Abstract

One way to maintain the security of data or information that is by using cryptographic methods. The rise of data breaches though it was secured by cryptography has happened lately. This research designed a new algorithm by using the steps hopscotch game and measures hopscotch game with gacuk already thrown in the first box. Algorithms designed in this research prove the pattern of the hopscotch game qualify five-tuple (Five-tuple) to design new algorithms. This research able to compare the speed of the process of randomness between hopscotch, Horse Sumba and AES-128. The comparison with the speed of horse Sumba and AES-128, the design based engklek step faster with an average of 0.120279647 seconds encryption and decryption process 0.085047639 seconds.

Keywords: Cipher Block, Cryptography, steps hopscotch game.

Abstrak

Salah satu cara untuk menjaga keamanan data atau informasi yaitu dengan menggunakan metode kriptografi. Maraknya pembobolan data meski sudah diamankan dengan kriptografi telah terjadi belakangan ini. Penelitian ini merancang algoritma baru dengan menggunakan langkah permainan engklek dan langkah permainan engklek dengan gacuk yang sudah dilempar di kotak pertama. Algoritma yang dirancang di penelitian ini membuktikan pola dalam permainan engklek memenuhi syarat lima-tuple (Five-tuple) untuk merancang algoritma baru. Penelitian ini dapat membandingkan kecepatan proses keacakan antara Engklek, Kuda Sumba dan AES-128. Hasil perbandingan kecepatan dengan Kuda Sumba dan AES-128, rancangan berbasis langkah engklek lebih cepat dengan rata-rata proses enkripsi 0,120279647 detik dan proses dekripsi 0,085047639 detik.

Kata Kunci: Cipher Blok, Kriptografi, Langkah Permainan Engklek.

¹⁾ Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

²⁾ Staf Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga.